

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

GLEN CARTER,

Plaintiff,

v.

NATIONAL SECURITY AGENCY,

Defendant.

:
:
:
:
:
:
:
:
:
:
:
:

Civil Action No. 12-0968 (CKK)

MEMORANDUM OPINION

This matter is before the Court on Defendant’s Motion for Summary Judgment [ECF No. 10].¹ For the reasons discussed below, the motion will be granted.

I. BACKGROUND

In February 2006, Plaintiff submitted a request to the National Security Agency (“NSA” or “Agency”) for the following information:

Information received from the Canadian authorities in the early nineties alerting [NSA] and calling for concern letters I am suspected of having written to a television Christian ministry.

¹ Also before the Court are “Plaintiff’s Memorandum of Points and Authorities in Support of his Cross-Motion for Summary Judgment” and “Plaintiff’s Memorandum of Points and Authorities in Support of His Reply to Defendant’s Motion for Summary Judgment” [ECF No. 19]. These documents do not comply in form and substance with Rule 56 of the Federal Rules of Civil Procedure and Local Civil Rule 7(h), and Plaintiff’s cross-motion for summary judgment will be denied. Instead, the Court construes these submissions together as Plaintiff’s opposition to Defendant’s Motion for Summary Judgment (“Pl.’s Opp’n”), the page numbers of which are designated by ECF.

Information portraying me as a dangerous person or, in the alternative, a suspected terrorist.

Information relating to the cross border transfer of personal information of all descriptions to the United States.

Information relating to the interception of communications of all descriptions.

Information relating to the seeking of a remedy to a suspected criminal offence.

Information relating to the issuance of an order, adverse in effect, curtailing my civil liberties in Canada, Barbados and the United Kingdom.

Information relating to a restriction of my freedom of movement and the withholding of individual rights and freedoms under law.^[2]

Def.'s Mem. of P. & A. in Supp. of its Mot. for Summ. J., Decl. of Diane M. Janosek ("Janosek Decl."), Ex. 1 (Letter to NSA, Attn: FOIA/PA Office, from Plaintiff dated February 14, 2006) at 2; *see* Compl. at 2–3 (page numbers designated by ECF).³ NSA processed the request under the Freedom of Information Act ("FOIA"), *see* 5 U.S.C. § 552. Janosek Decl. ¶ 9 n.1.⁴

² Plaintiff apparently wrote letters "to a television Christian Ministry" in the United States, and he believes that personal information about him has been "exported from Canada via the Canadian authorities (Royal Canadian Mounted Police, Canadian Security Service Intelligence Agency) via Interpol Ottawa to the Central Intelligence Agency," subsequently "transferred from the Central Intelligence Agency to the National Security Agency," resulting in the "invasion of [his] personal privacy through technological methods employed by US, Canadian and British authorities." Def.'s Mem. of P. & A. in Supp. of its Mot. for Summ. J., Decl. of Diane M. Janosek, Ex. 3 (Appeal under Freedom of Information Act, 5 U.S.C. sect. 552, As Amended By Public Law No. 104-231, 110 Stat. 3048) at 2. Allegedly "writ[ten] during a very difficult phase of [Plaintiff's] life," these letters "criticized the US, the media and corporate America," and "later broadened in scope to encompass and address other social issues." *Id.*, Ex. 3 at 6. Plaintiff "never intended to cause public harm and dismay." Compl. at 5.

³ The Court construes Plaintiff's "Petition for Review" and the attached "Plaintiff's Memorandum in Appeal of Administrative's [sic] Agency's Internal Appeal Decision of September 14, 2006," together as a civil complaint ("Compl.").

⁴ NSA declined to process the request under the Privacy Act, *see* 5 U.S.C. § 552a, because the Privacy Act applies only to United States citizens. Janosek Decl. ¶ 9 n.1. Plaintiff has identified himself as "a Canadian citizen who has retained British citizenry (a dual citizen, that is)." Pl.'s Opp'n at 1.

“To the extent that Plaintiff’s request could be considered a request for intelligence information,” NSA treated it as one “for records on the surveillance, targeting, and/or domestic collection of [information pertaining to Plaintiff] by NSA.” Janosek Decl. ¶ 9. Relying on Exemptions 1 and 3, NSA denied the request in its entirety and explained its reasons as follows:

We have determined that the fact of the existence or non-existence of the materials you request is a currently and properly classified matter in accordance with Executive Order 12958, as amended. Thus, your request is denied pursuant to the first exemption of the FOIA which provides that the FOIA does not apply to matters that are specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign relations and are, in fact[,] properly classified pursuant to such Executive Order.

In addition, this Agency is authorized by various statutes to protect certain information concerning its activities. The third exemption of the FOIA provides for the withholding of information specifically protected from disclosure by statute. Thus, your request is also denied because the fact of the existence or non-existence of the information is exempted from disclosure pursuant to the third exemption. The specific statutes applicable in this case are Title 18 U.S. Code 798; Title 50 U.S. Code 403-1(i); and Section 6, Public Law 86-36 (50 U.S. Code 402 note).

Id., Ex. 2 (Letter to Plaintiff from Louis F. Giles, Director of Policy, NSA, dated April 20, 2006, regarding FOIA Case No. 48604) at 2.

Plaintiff filed an administrative appeal of NSA’s initial determination on June 19, 2006. *See generally id.*, Ex. 3 (Appeal under Freedom of Information Act, 5 U.S.C. sect. 552, As Amended By Public Law No. 104-231, 110 Stat. 2048). NSA acknowledged its receipt of the appeal on August 3, 2006. *Id.*, Ex. 4 (Letter to Plaintiff from Ariane E. Cerlenko, Associate General Counsel, NSA, regarding Case No. 48604/Appeal No. 3145, dated August 3, 2006). NSA’s initial determination was affirmed, and it was determined that “the appropriate response

to [Plaintiff's] request is to continue to neither confirm nor deny the existence or non-existence of the materials . . . request[ed].” *Id.*, Ex. 5 (Letter to Plaintiff from John Inglis, Freedom of Information Act/Privacy Act Appeals Authority, dated September 14, 2006) at 2. The affirmance was explained in part as follows:

Regardless of whether NSA has records related to you, or any individual, NSA can neither confirm nor deny alleged activities or targets. To do otherwise when challenged under the FOIA would result in the exposure of intelligence information, sources, and methods and would severely undermine surveillance activities in general. For example, if NSA denied allegations about intelligence activities or targets in cases where such allegations were false (e.g., we told one FOIA requester that we had no records), but remained silent in cases where the allegations were accurate, it would tend to reveal that the individuals in the latter cases were targets. Any further elaboration concerning these matters would reveal information that is currently and properly classified under Executive Order 12958, as amended.

Id.

Plaintiff challenges this administrative appeal decision “refusing him access to personal information believed to be contained in intelligence records.” Compl. at 2. He alleges that NSA “failed to properly invoke a Glomar [response] and to properly support this response with applicable statutes . . . by properly stating the precise grounds on which access to responsive records, if any, was denied.”⁵ *Id.* at 3. According to Plaintiff, the issues presented are:

(a) did NSA properly rely on the exempt provisions of FOIA, (b) was a Glomar response standard of refusal . . . appropriate to the categories of personal information requested, (c) did the Agency make proper use of the general exemption review standards

⁵ A Glomar response “takes its name from the *Hughes Glomar Explorer*, a ship built (we now know) to recover a sunken Soviet submarine, but disguised as a private vessel for mining manganese nodules from the ocean floor.” *Elec. Privacy Info. Ctr. v. Nat’l Sec. Agency*, 678 F.3d 926, 931 n.2 (D.C. Cir. 2012) (quoting *Bassiouni v. CIA*, 392 F.3d 244, 246 (7th Cir. 2004) (internal quotation marks omitted)). As is discussed below, an agency providing a Glomar response neither confirms nor denies the existence of information responsive to a FOIA request. See *Gardels v. CIA*, 689 F.2d 1100, 1103 (D.C. Cir. 1982).

established in non Glomar cases, and (d) did the Agency properly meet the burden of proof required of it in order to sustain its action.

Id.

II. DISCUSSION

A. Summary Judgment in a FOIA Case

“FOIA cases typically and appropriately are decided on motions for summary judgment.” *Defenders of Wildlife v. U.S. Border Patrol*, 623 F. Supp. 2d 83, 87 (D.D.C. 2009). The Court will grant summary judgment if the movant shows that there is no genuine dispute as to any material fact and is entitled to judgment as a matter of law. *See* Fed. R. Civ. P. 56(a). In a FOIA action to compel production of agency records, the agency “is entitled to summary judgment if no material facts are in dispute and if it demonstrates ‘that each document that falls within the class requested either has been produced . . . or is wholly exempt from the [FOIA’s] inspection requirements.’” *Students Against Genocide v. Dep’t of State*, 257 F.3d 828, 833 (D.C. Cir. 2001) (quoting *Goland v. CIA*, 607 F.2d 339, 352 (D.C. Cir. 1978)).

Summary judgment may be based solely on information provided in an agency’s supporting affidavits or declarations if they are relatively detailed and when they describe “the documents and the justifications for nondisclosure with reasonably specific detail, demonstrate that the information withheld logically falls within the claimed exemption, and are not controverted by either contrary evidence in the record [or] by evidence of agency bad faith.” *Military Audit Project v. Casey*, 656 F.2d 724, 738 (D.C. Cir. 1981). “To successfully challenge an agency’s showing that it complied with the FOIA, the [P]laintiff must come forward with ‘specific facts’ demonstrating that there is a genuine issue with respect to whether the agency has

improperly withheld extant agency records.” *Span v. U.S. Dep’t of Justice*, 696 F. Supp. 2d 113, 119 (D.D.C. 2010) (quoting *Dep’t of Justice v. Tax Analysts*, 492 U.S. 136, 142 (1989)).

In a FOIA case, the Court determines *de novo* whether an agency properly withholds information under a claimed exemption. *See, e.g., King v. U.S. Dep’t of Justice*, 830 F.2d 210, 217 (D.C. Cir. 1987). This is so even if national security matters are at issue. *See Halperin v. CIA*, 629 F.2d 144, 148 (D.C. Cir. 1980). Deference is accorded, however, to an agency’s expertise in national security matters. *See, e.g., Taylor v. Dep’t of the Army*, 684 F.2d 99, 109 (D.C. Cir. 1982) (accorded “utmost deference” to classification affidavits); *Goland*, 607 F.2d at 352.

B. SIGINT and the NSA’s National Security Mission

The NSA’s declarant explains that the Agency is “a separately organized agency within the Department of Defense under the direction, authority, and control of the Secretary of Defense.” Janosek Decl. ¶ 4. Its “foreign intelligence mission includes the responsibility to collect, process, analyze, produce, and disseminate signals intelligence (SIGINT) information, of which communications intelligence (COMINT) is a significant subset, for (a) national foreign intelligence purposes, (b) counterintelligence purposes, and (c) the support of military operations.” *Id.* NSA performs its SIGINT mission by “exploit[ing] foreign electromagnetic signals to obtain intelligence information necessary for the national defense, national security, or conduct of foreign affairs.” *Id.* ¶ 5. The declarant further explains that, through “a sophisticated worldwide SIGINT collection network,” the Agency “acquires, among other things, foreign and international electromagnetic communications.” *Id.* The technological infrastructure supporting

these efforts, she states, “has taken years to develop at the cost of billions of dollars and untold human effort,” and it “relies on sophisticated collection and processing technology.” *Id.*

Intelligence information is gathered and analyzed for two main purposes: “to direct United States resources as necessary to counter threats” and “to direct the foreign policy of the United States.” *Id.* ¶ 6. The declarant states that “intelligence produced by NSA is often unobtainable by other means.” *Id.* Such information is distributed to the President of the United States, various senior government officials, military departments and law enforcement agencies, and it may include information relevant to “military order of battle[,] threat warnings and readiness[,] arms proliferation[,] terrorism[,] and foreign aspects of international narcotics trafficking.” *Id.* The declarant further states that “NSA’s ability to produce foreign intelligence information depends on its access to foreign and international electronic communications.” *Id.* ¶ 7. The technology used in these processes “is both expensive and fragile,” and “[p]ublic disclosure of either the capability to collect specific communications or the substance of the information itself can easily alert targets to the vulnerability of their communications.” *Id.*

C. Interpretation of Plaintiff’s FOIA Request

The NSA treated Plaintiff’s FOIA request as if it “encompass[ed] a request for information regarding whether [Plaintiff] was a target of NSA’s surveillance efforts.” Janosek Decl. ¶ 11; *see id.* ¶ 9. According to Plaintiff, the NSA “erred right from the start by misunderstanding and misinterpreting this request for something other than that which was intended by the Plaintiff, by assuming that his request was a request for records on *surveillance*, *targeting*, and the *domestic collection* of responsive records.” Pl.’s Mem. of P. & A. in Supp. of his Cross-Mot. for Summ. J. (“Pl.’s Opp’n”) at 4 (emphasis in original); *see id.* at 7. His request

“refer[red] to ‘information’ and not [‘]intelligence information’ per se.” *Id.* at 4. According to Plaintiff, “both NSA and the CIA have been collecting and processing personal information on him not on national security grounds for a Glomar response to have effect but out of service to special media interests.” *Id.* “Only 1/7th of [his] access request (item[] No. 4, that is) related to the Plaintiff possibly being the target of surveillance activities conducted by NSA whilst the other aspects to it refer to personal information which would ordinarily fall outside the scope of Exemptions 1 and 3,” such that a “Glomar response should in no way be used” with respect to the other six items listed in his request. *Id.* at 12.

By means of this FOIA request, Plaintiff seeks “personal information believed to be caught up in intelligence records believed to be in the custody, control and management of the Agency.” *Id.* at 1. He apparently is under the impression that NSA not only is able to separate out “personal” information from all the information that the Agency would have or could have acquired only through SIGINT, but also is required do so. In light of the origin, function, and mission of the NSA, it is reasonable for its staff to have interpreted Plaintiff’s FOIA request as one for information about him which the Agency obtained in the course of its communications surveillance activities. After all, Plaintiff did seek “[i]nformation relating to the interception of communications of all descriptions.” Janosek Decl., Ex. 1 (FOIA request). And for the reasons discussed below, NSA’s Glomar response is appropriate.

D. Exemption 1

Exemption 1 protects matters that are “(A) specifically authorized under criteria established by an Executive [O]rder to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive [O]rder[.]” 5 U.S.C. §

552(b)(1). Pursuant to Executive Order 13,526, 75 Fed. Reg. 707 (Dec. 29, 2009), information may be classified only if all of the following conditions are met:

- (1) an original classification authority is classifying the information;
- (2) the information is owned by, produced by or for, or is under the control of the United States Government;
- (3) the information falls within one or more of the categories of information listed in section 1.4 of this order; and
- (4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage.

Id. § 1.1(a). Information may be classified either at the “top secret,” “secret,” or “confidential” level, *id.* § 1.2(a), and such classified information must fall within one of the following categories:

- (a) military plans, weapons systems, or operations;
- (b) foreign government information;
- (c) *intelligence activities (including covert action), intelligence sources or methods, or cryptology;*
- (d) foreign relations or foreign activities of the United States, including confidential sources;
- (e) scientific, technological, or economic matters relating to the national security;
- (f) United States Government programs for safeguarding nuclear materials or facilities;
- (g) *vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security;* or
- (h) the development, production, or use of weapons of mass destruction.

Id. § 1.4 (emphasis added).⁶

The declarant, who is a “TOP SECRET original classification authority,” Janosek Decl. ¶ 2, explains that “[c]onfirming the existence or nonexistence of responsive records would disclose information that is currently and properly classified TOP SECRET . . . because such a positive or negative response could reasonably be expected to cause exceptionally grave damage to national security,” *id.* ¶ 14. She further explains:

Confirmation by NSA that a person’s activities are not of a foreign intelligence interest or that NSA is unsuccessful in collecting foreign intelligence information in [his] activities on a case-by-case basis would allow our adversaries to accumulate information and draw conclusions about the NSA’s technical capabilities, sources, and methods. NSA’s adversaries would have a roadmap instructing them as to which communication modes and personnel remain safe or are successfully defeating NSA’s capabilities. For example, if NSA were to admit publicly in response to [a FOIA] request that no information about Persons X, Y, and Z exist, but in response to a separate . . . request about Person T state only that the Agency can neither confirm nor deny the existence of such

⁶ The Agency initially relied on Executive Order No. 12,958, 60 Fed. Reg. 19825 (Apr. 17, 1995), which in relevant part read:

(c) intelligence activities (including special activities), intelligence sources or methods, or cryptology; . . .

(g) vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security.

Id. § 1.5. Executive Order 12,958 “has since been revoked and replaced by Executive Order 13[,]526” Janosek Decl. ¶ 9 n.2.

“[A] reviewing court [assesses] the propriety of a classification decision purportedly supporting an Exemption 1 claim in terms of the [E]xecutive [O]rder in force at the time the agency’s ultimate classification decision is actually made.” *King*, 830 F.2d at 217. The declarant does not provide the date on which NSA made its initial classification decision. The language of subparagraphs (c) and (g) of both Executive Orders is substantially similar, and the Court finds that the classified information at issue in this case falls within the scope of either Order.

records, this would give rise to the inference that Person T is a target of NSA's surveillance efforts. These inferences would disclose the targets and capabilities (*i.e.* NSA's sources and methods) of NSA's SIGINT activities and functions and inform our adversaries of the degree to which NSA is aware of some of their operatives or is able to successfully exploit particular communications.

Id. For these reasons, NSA invokes Exemption 1 and offers only a Glomar response because “the fact of the existence or nonexistence of the intelligence information requested by Plaintiff is a currently and properly classified matter in accordance with Executive Order 13[,]526, as amended.” *Id.*

E. Exemption 3

Exemption 3 protects records that are “specifically exempted from disclosure by statute . . . provided that such statute (A) [requires withholding] in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld.” 5 U.S.C. § 552(b)(3). It “differs from other FOIA exemptions in that its applicability depends less on the detailed factual contents of specific documents; the sole issue for decision is the existence of a relevant statute and the inclusion of withheld material within that statute’s coverage.” *Goland*, 607 F.2d at 350; *Ass’n of Retired R.R. Workers v. U.S. R.R. Ret. Bd.*, 830 F.2d 331, 336 (D.C. Cir. 1987). In other words, NSA “need only show that the statute claimed is one of exemption as contemplated by Exemption 3 and that the withheld material falls within the statute.” *Larson v. Dep’t of State*, 565 F.3d 857, 868 (D.C. Cir. 2009) (citing *Fitzgibbon v. CIA*, 911 F.2d 755, 761-62 (D.C. Cir. 1990)).

NSA’s declarant explains that “any confirmation or denial that Plaintiff has been or is a target is precluded by three statutes.” Janosek Decl. ¶ 11. First, NSA relies on Section 6 of the National Security Agency Act of 1959, which in relevant part provides:

[N]othing in [the National Security Agency Act of 1959] or any other law . . . shall be construed to require the disclosure of the organization or any function of the [NSA], or any information with respect to the activities thereof, or the names, titles, salaries, or number of persons employed by such agency.

50 U.S.C. § 402 (note).⁷ Second, NSA relies on 18 U.S.C. § 798, under which a person who knowingly and willfully discloses to an unauthorized person “any classified information . . . concerning the communication intelligence activities of the United States . . . or . . . obtained by the processes of communication intelligence from the communications of any foreign government, knowing the same have been obtained by such processes,” commits a criminal offense punishable by a fine or a maximum prison term of ten years or both. 18 U.S.C. § 798(a)(3), (4). Third, NSA relies on Section 102(A)(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, which provides that “[t]he Director of National Intelligence *shall* protect intelligence sources and methods from unauthorized disclosure.” 50 U.S.C. § 403-1(i)(1) (emphasis added).⁸ It is settled that these statutes are among those contemplated by Exemption 3. *See Am. Civil Liberties Union v. U.S. Dep’t of Defense*, 628 F.3d 612, 619 (D.C. Cir. 2011) (recognizing prior holding that “the National Security Act, which also authorizes the Executive to withhold ‘intelligence sources and methods’ from public disclosure, 50 U.S.C. § 403-1(i)(1), qualifies as an exemption statute under [E]xemption 3”); *Larson*, 565 F.3d at 868 (recognizing that 18 U.S.C. § 798 qualifies as an Exemption 3 statute).

The declarant asserts that the “release of any confirmation or denial that Plaintiff has been or is a target is precluded by . . . statute[.]” Janosek Decl. ¶ 11. For this reason, NSA takes the position that “the existence or nonexistence of [the information Plaintiff requests] is exempt

⁷ This section of the National Security Agency Act of 1959, which formerly appeared as a note to 50 U.S.C. § 402, may now be found at 50 U.S.C. § 3605(a).

⁸ This section of the Intelligence Reform and Terrorism Prevention Act of 2004, which formerly appeared at 50 U.S.C. § 403-1, may now be found at 50 U.S.C. § 3024(i)(1).

from disclosure pursuant to Exemption[] . . . 3 of the FOIA.” *Id.* The three statutes on which NSA relies, the declarant states, are designed “to protect the fragile nature of NSA’s SIGINT efforts to include, but not limited to, the existence and depth of signals intelligence-related successes, weaknesses, and exploitation techniques.” *Id.* ¶ 20. “These statutes recognize the vulnerability of signals intelligence to countermeasures and the significance of the loss of valuable intelligence information to national policy makers and the Intelligence Community.” *Id.* Where “Congress specifically prohibited the disclosure of information related to NSA’s functions and activities and its communications intelligence activities, as well as the sources and methods used by the Intelligence Community as a whole,” the declarant concludes that “NSA’s SIGINT activities and functions, and its intelligence sources and methods[,] would be revealed if any of the withheld information about NSA’s collection were disclosed,” if any such information exists. *Id.* “[A]cknowledgement of the existence or nonexistence of intelligence information relating to Plaintiff is prohibited by statute” and thus, concludes the declarant, is “exempt from disclosure” under FOIA. *Id.* ¶ 21.

F. Plaintiff’s Objections

Plaintiff raises a handful of objections, none of which establishes the existence of a genuine issue of material fact in dispute with respect to NSA’s compliance with the FOIA.

First, Plaintiff attacks the sufficiency of NSA’s supporting declaration. With respect to NSA’s reliance on Exemption 1, Plaintiff “denies that the withheld information substantively falls within the scope of Executive Order 13526.” Pl.’s Opp’n at 7. According to Plaintiff, “NSA’s response presupposes that every person on whom foreign intelligence is shared is [a] surveillance target,” *id.*, even though “not all foreign intelligence received by NSA may have the

credibility to even come close to be considered surveillance information.” *id.* at 8. He further disputes NSA’s assertion that revelation of the Agency’s “capability to collect specific communications . . . can so easily alert a surveillance target to the vulnerability of [his] communications.” *Id.* Plaintiff deems this notion an “exceptional stretch of one’s imagination” and dismisses the argument as having “no real merit.” *Id.* With respect to Exemption 3, while Plaintiff does not dispute the content or purpose of the three statutes on which NSA relies, he argues that the statutes are not designed “to unjustifiably excuse the [Agency] from providing a proper response under FOIA.” *Id.* at 9. He sees no reason why NSA cannot protect its “raw data,” *id.*, while disclosing to him a “final outcome” which withholds any sensitive information that is not personal to him, *id.* For example, Plaintiff posits that “a set of operations is performed on signals intelligence so as to provide a refined, reproducible product to work with” and that he is entitled to the finished product “after all irrelevant information such as methods and techniques relating to national defence [sic] ha[ve] been stripped away,” *id.* at 8., without posing a risk to national security, *see id.* at 9.

The Agency’s declaration is “presumed to be in good faith,” and a requester “can rebut this presumption with evidence of bad faith.” *Elec. Privacy Info. Ctr. v. Dep’t of Homeland Sec.*, 384 F. Supp. 2d 100, 107 (D.D.C. 2005) (citing *SafeCard Servs., Inc. v. SEC*, 926 F.2d 1197, 1200 (D.C. Cir.1991)). Plaintiff offers nothing more than opinion and speculation as to the deficiencies in the declaration, and therefore does not undermine the deference normally afforded to an agency, and particularly in the realm of national security matters. *See Friedman v. U.S. Secret Service*, No. 06-2125, 2013 WL 588288, at *14 (D.D.C. Feb. 14, 2013) (finding that, for Exemption 1, Plaintiff’s “speculation as to the declarants’ bad faith does not overcome the deference generally accorded to agency declarations.”).

Nor does Plaintiff demonstrate any other basis to conclude that NSA's Glomar response, which is "an exception to the general rule that agencies must acknowledge the existence of information responsive to a FOIA request and provide specific, non-conclusory justifications for withholding that information," *Roth v. U.S. Dep't of Justice*, 642 F.3d 1161, 1178 (D.C. Cir. 2011), is not proper in this case. If there were any personal information about Plaintiff in NSA's records, its very existence—without more—reveals classified intelligence information. Here, NSA refuses to confirm or deny the existence or nonexistence of the information Plaintiff requests because Exemptions 1 and 3 "would . . . preclude the acknowledgement of such documents." *Elec. Privacy Info. Ctr. v. NSA*, 678 F.3d 926, 931 (D.C. Cir. 2012); *see Wilner v. NSA*, 592 F.3d 60, 70 (2d Cir. 2009) (stating that a Glomar response is "applicable in cases where to answer the FOIA inquiry would cause harm cognizable under a [] FOIA exception—in other words, in cases in which the existence or nonexistence of a record is a fact exempt from disclosure under a FOIA exception") (quoting *Gardels v. CIA*, 689 F.2d 1100, 1103 (D.C. Cir. 1982) (internal quotation marks omitted)), *cert. denied*, 131 S. Ct. 387 (2010). "When the Agency's position is that it can neither confirm nor deny the existence of the requested records, there are no relevant documents for the court to examine other than the affidavits which explain the Agency's refusal." *Phillippi v. CIA*, 546 F.2d 1009, 1013 (D.C. Cir. 1976).

NSA establishes that any further response to Plaintiff's FOIA request would result in disclosure of intelligence information which, in light of the NSA's intelligence responsibilities, amounts to the disclosure of the sources of and methods by which its intelligence is collected. *See Bassiouni v. CIA*, 392 F.3d 244, 245 (7th Cir. 2004) (affirming a Glomar response to a first-person request for CIA records on the ground that "providing a list of the documents that mention [the requester], and claiming document-by-document exemptions for those whose

contents are classified, would reveal details about intelligence-gathering methods,” even if “disclosure could be innocuous”); *People for the Am. Way Found. v. NSA/Cent. Sec. Serv.*, 462 F. Supp. 2d 21, 31 (D.D.C. 2006) (concluding that the NSA’s Glomar response to a request for records related to surveillance of Plaintiff was appropriate because confirmation that a person’s activities are not of foreign intelligence interest or that the NSA was unable to collect foreign intelligence information on his activities “would allow our adversaries to accumulate information and draw conclusions about NSA’s technical capabilities, sources, and methods”); *see also Wolf v. CIA*, 473 F.3d 370, 376 (concluding that revealing the existence of CIA records “regarding specific foreign nationals could potentially reveal targets of CIA surveillance and, thus, CIA methods” by “signal[ing] to a foreign intelligence service the specific persons and areas in which the CIA is interested and upon which it focuses its methods and resources”). Further, the Agency establishes that any such information is classified in accordance with Executive Order 13,526, and is otherwise protected from release by the relevant provisions of the National Security Act of 1959, 18 U.S.C. § 798, and the Intelligence Reform and Terrorism Prevention Act of 2004.

III. CONCLUSION

The Court concludes that there are no genuine issues of material fact in dispute as to the NSA’s compliance with the FOIA, and that the NSA is entitled to judgment as a matter of law. Accordingly, Defendant’s motion for summary judgment will be granted. An Order accompanies this Memorandum Opinion.

DATE: August 26, 2013

COLLEEN KOLLAR-KOTELLY
United States District Judge